

ABSTRACT OF THE DISCLOSURE

Problem

The invention aims at preventing burglary use of a burglary-use preventing subject such as a credit card or portable phone.

Solution for Problem

A reporting electronic station is provided to the Internet. A mail address of a legitimate right holder of a burglary-use preventing subject is registered at the electronic station. If such a burglary-use preventing subject as a credit card or portable phone is used, a computer at a banking organ or telephone company transmits an e-mail through the Internet to a mail address of the legitimate right holder of the burglary-use preventing subject related to this use. The information of this e-mail for that mail address received at the electronic station is in turn received by a beeper communication center. The beeper communication center displays the contents of the e-mail (fact that the credit card, portable phone, etc. has been used) at a display portion of a beeper of the legitimate right holder.

[0008]

FIG. 1 is a configuration diagram for showing a burglary-use preventing system related to one embodiment of the invention. This burglary-use preventing system has a

configuration in which an e-mail network, a paging network, and a computer of a bank or telephone company are interconnected in a wired or wireless communication. The e-mail network is mainly comprised of the Internet, in which is provided a reporting e-mail station (INT) which provides a burglary-use preventing e-mail server, which is detailed later. The page network constitutes a pager communication network, in which when a burglary-use preventing e-mail is sent to the reporting e-mail station (INT), the paging center (PP) receives a report of the contents of this burglary-use preventing e-mail from the reporting e-mail station (INT). Then, the paging center (PP) reports to a pager which corresponds to an address of this burglary-use preventing e-mail to thereby ring the beeper and also display the contents of the burglary-use preventing e-mail at the display portion.

[0009]

One example is described, in which a credit card of Mr. M, who is the legitimate right holder thereof, is inserted into this burglary-use preventing system. Suppose that a domain name of the reporting e-mail station (INT) provided in the Internet is "YYYY.COM" and a reporting address of Mr. M is "CCC", an address of his burglary-use preventing e-mail is "CCC@YYYY.COM". Also, a beeper A of Mr. M is user-registered as a beeper that can be reported from the paging network so that it may correspond to that reporting address "CCC".

[0010]

When Mr. M or any one of his family members used his credit card, both use of this credit card and a paid amount are reported to a computer of bank E, which computer automatically transmits his burglary-use preventing e-mail to the Internet. The contents of the e-mail include a symbol indicating a type of the credit card (e.g., VISA, Master), a code No. of bank E, and a paid amount expressed in units of a predetermined currency value; for example, the contents of [A04]20000 are accompanied by the address "CCC@YYY.COM" and sent to the Internet.

[0011]

The e-mail thus sent to the Internet is then sent to a server having that domain name. This burglary-use preventing e-mail destined to Mr. M immediately arrives at the reporting e-mail station (INT), which in turn notifies the paging center (PP) of a report that the contents of [A04]20000 for the address CCC have arrived at it. The paging center (PP) calls the beeper A of Mr. M indicated by the address CCC to transmit the e-mail contents of [A04]20000 at the display portion of the beeper A.

[0012]

When Mr. M sees contents displayed at the beeper A rung after transaction of his credit card, he can confirm the transaction of the credit card by himself or one of his family members was that by use of the VISA card (symbol A) and the bank was an XX bank with a code No. of 04, and an amount was 20000 Wen (Chinese currency) and also that this burglary-use preventing system is operating properly.

[0013]

Even when some one else stole his credit card and used it fraudulently in transaction, similarly, the information is transmitted to the beeper A of Mr. M. By seeing the contents displayed at his beeper A when it was rung, Mr. M can immediately know a fact that his credit card was stolen and currently used fraudulently. Then, he can report to the police and also request the card company to disable the credit card.

[0014]

Although the above-mentioned embodiment has been of prevention of burglary use of a credit card, it may be of prevention of burglary use of a portable phone by means of the same burglary-use prevention system. Suppose here that Mr. N or one of his family members used his portable phone to make a phone call. In this case, a computer F of the telephone company automatically transmits e-mail contents [-222-] indicating the current use of that portable phone to the Internet at his burglary-use prevention e-mail address "DDD@YYYY.COM" specified by the company itself. This e-mail goes through the communication network of the Internet and finally arrives at the e-mail station (INT: domain name YYYY.COM), which is the reporting server for burglary-use prevention. The paging center (PP) receives a report from the reporting e-mail station (INT) to then call a beeper B of Mr. N, thus displaying at its display portion [-222-], which indicates that his portable phone is currently used. When Mr. N sees the contents displayed his beeper B immediately after

he used his portable phone, he can confirm that the burglary-use prevention system is operating properly.

[0015]

Even when some one else stole the portable phone of Mr. N and used it to make a phone call, similarly, its current use is displayed at his beeper B. By seeing the displayed contents, Mr. N can immediately know that his portable phone was stolen and used, to report it to the police and also request the telephone company to disable that stolen portable phone.

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-163030

(43) 公開日 平成9年(1997)6月20日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 M 11/04			H 0 4 M 11/04	
G 0 8 B 15/00		0234-2E	G 0 8 B 15/00	
H 0 4 Q 7/06			H 0 4 M 3/42	1 0 2
7/08			H 0 4 B 7/26	1 0 3 A
7/12		9466-5K	H 0 4 L 11/20	1 0 1 B
審査請求 未請求 請求項の数 6 F D (全 6 頁) 最終頁に続く				

(21) 出願番号 特願平8-257579

(22) 出願日 平成8年(1996)9月5日

(31) 優先権主張番号 95117081.3

(32) 優先日 1995年10月26日

(33) 優先権主張国 中国 (CN)

(71) 出願人 598141480

ウォン カム フー

黄 金富

香港 沙田 徑口路 1-3 號

(72) 発明者 ウォン カム フー

香港 沙田 徑口路 1-3 號

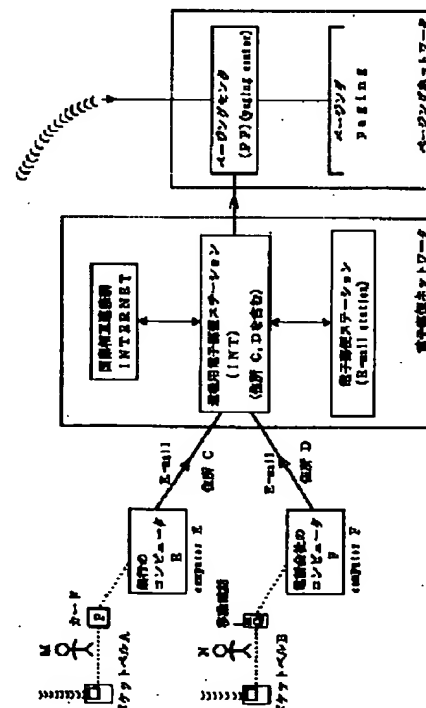
(74) 代理人 弁理士 山本 喜幾

## (54) 【発明の名称】 盗用防止方法およびそのシステム

## (57) 【要約】

【課題】 クレジットカードや携帯電話等の盗用防止対象物の盗用を防止する。

【解決手段】 インターネットに、通報用の電子ステーションを設ける。盗用防止対象物の正当権利者のメールアドレスを、電子ステーション内に登録する。クレジットカードや携帯電話等の盗用防止対象物が使用されたとき、金融機関のコンピュータや電話会社のコンピュータ等から当該使用に係る盗用防止対象物の正当権利者のメールアドレス宛てに電子メールをインターネット経由で送信する。電子ステーションが受信したメールアドレス宛ての電子メールの情報を、ポケットベル通信センタが受取る。ポケットベル通信センタは、電子メールの内容(クレジットカードや携帯電話等の使用の事実)を、正当権利者が保持するポケットベルの表示部に表示させる。



## 【特許請求の範囲】

【請求項1】 コンピュータネットワークを介して処理されるべき盗用防止対象物が該コンピュータを通じて使用された場合に、該使用に関わるコンピュータは、前記コンピュータネットワークに関連する電子郵便ネットワークに予め設定した前記盗用防止対象物の正当権利者のメールアドレスへ該盗用防止対象物の使用状況の情報に関する電子メールを送信し、電子郵便ネットワークに予め設定したサーバは、この電子メールを受信すると直ちにポケットベル通信網のセンタに前記電子メールにおける使用状況の情報を通報し、前記ポケットベル通信網のセンタは、前記サーバからの通報を受けることにより、前記電子メールのメールアドレスにより特定される前記正当権利者が所持するポケットベルを呼出すと共に、該ポケットベルの表示部に前記盗用防止対象物の使用状況の情報を表示するようにしたことを特徴とする盗用防止方法。

【請求項2】 前記盗用防止対象物として、クレジットカード、小切手、マネーカード、携帯電話の何れかが挙げられる請求項1記載の盗用防止方法。

【請求項3】 前記電子郵便ネットワークとしてインターネットを利用し、Eメールで前記電子メールを送信するようにした請求項1記載の盗用防止方法。

【請求項4】 コンピュータネットワークを介して処理されるべき盗用防止対象物が使用された場合に、該コンピュータネットワークに関連する電子郵便ネットワーク内の該盗用防止対象物の正当権利者宛に予め設定されたメールアドレスへ、前記盗用防止対象物の使用状況の情報に関する電子メールを発信する前記使用に関わるコンピュータと、前記電子郵便ネットワーク内に設けられ、前記盗用防止対象物の使用状況の情報に関する電子メールを受信するよう予め設定されたサーバと、前記電子メールを受信した前記サーバから通報を受け、該電子メールのメールアドレスにより特定される前記正当権利者の所持するポケットベルを呼出すと共に、該ポケットベルの表示部に前記盗用防止対象物の使用状況の情報を表示するポケットベル通信網のセンタとから構成したことを特徴とする盗用防止システム。

【請求項5】 前記盗用防止対象物として、クレジットカード、小切手、マネーカード、携帯電話の何れかが挙げられる請求項4記載の盗用防止システム。

【請求項6】 前記電子郵便ネットワークはインターネットであり、前記電子メールはEメールである請求項4記載の盗用防止システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 この発明は、クレジットカードや携帯電話等の盗用防止方法およびそのシステムに関し、更に詳細には、コンピュータネットワークを介して

クレジットカード等に代表される盗用防止対象物が使用されたとき、該盗用防止対象物の使用の事実をインターネットとポケットベルを用いて正当権利者に直ちに通知し得るようにした盗用防止方法およびそのシステムに関するものである。

## 【0002】

【従来の技術】 電子技術の発展は目覚ましく、経済活動においては、現金の授受よりもクレジットカードやマネーカードを用いた取引の方が多くなってきている。また、電話機も有線式の据置式のものよりも、無線式の携帯型のものが増えてきている。そして、人間の経済活動は、通信回線とコンピュータを結合したネットワークシステムの中で行なわれる方向にある。

## 【0003】

【発明が解決しようとする課題】 コンピュータと通信技術とが結合したネットワークシステムでは、今後益々、クレジットカード等による取引が増大し、通信も携帯電話が使われる傾向にある。そこで問題となるのが、クレジットカードや携帯電話の不正な使用すなわち盗用である。クレジットカード等の磁気記憶情報媒体による取引は、現金取引に比べて手軽であり、かつ全世界的なコンピュータネットワークを介するものであるために、これが盗用されると一挙に多額の損害を蒙る慮がある。また携帯電話も盗用されると、これにより多額の通話料金が正当権利者に請求されることになる。

## 【0004】

【発明の目的】 この発明は、前述した欠点に鑑み、これを好適に解決するべく提案されたものであって、コンピュータネットワークを介したクレジットカードや携帯電話等が盗用されるのを防止する盗用防止方法およびそのシステムを提供することを目的とする。

## 【0005】

【課題を解決するための手段】 前記の目的は、インターネットに通報用の電子ステーションを設け、クレジットカードや携帯電話の正当権利者のメールアドレスをこの電子ステーション内に登録しておき、クレジットカードや携帯電話が使用されたとき、金融機関のコンピュータや電話会社のコンピュータ等から当該使用に係るクレジットカードや携帯電話等の正当権利者の前記メールアドレス宛てに電子メールをインターネット経由で送信し、前記電子ステーションが受信した前記メールアドレス宛ての電子メールの情報をポケットベル通信センタが受取り、ポケットベル通信センタは、該電子メールの内容（クレジットカードや携帯電話等の使用の事実）を正当権利者が保持するポケットベルの表示部に表示させることにより達成される。

【0006】 クレジットカードや携帯電話等の盗用防止対象物の正当権利者は、自らこれを使用したときや、自分の家族等その使用を認めている者が正当に使用したときには、自己の保有するポケットベルにその使用の事実

が表示されるので、盗用防止対象物の使用がなされた度にその確認を行なうことができる。逆に云えば、他人が例えばクレジットカードを盗用して不正に使用したときも、同様にポケットベルに表示されるために、該カードの正当権利者は盗用されたことを直ちに知ることができ、金融機関や電話会社に通報してそのクレジットカードの使用を停止させることができる。

#### 【0007】

【発明の実施の形態】次に、本発明に係る盗用防止方法およびそのシステムにつき、好適な実施例を挙げて、添付図面を参照しながら以下説明する。

【0008】図1は、本発明の一実施例に係る盗用防止システムの構成図である。この盗用防止システムは、電子郵便ネットワークと、ページングネットワークと、銀行のコンピュータや電話会社のコンピュータとを相互に無線或いは有線で接続することで構成される。電子郵便ネットワークはインターネットを主体とし、インターネット内に、詳細は後述する盗用防止用Eメールのサーバとなる通報用電子郵便ステーション(INT)を設けておく。ページングネットワークは、ポケットベル通信網を構成し、その中のページングセンタ(PP)は、通報用電子郵便ステーション(INT)に盗用防止用Eメールが送られてきたとき、この通報用電子郵便ステーション(INT)からその盗用防止用Eメールの内容が通報される。そして、ページングセンタ(PP)は、この盗用防止用Eメールのアドレスに対応したポケットベルに通報し、このポケットベルを鳴動させると共に盗用防止用Eメールの内容をその表示部に表示させる。

【0009】一例として、正当権利者であるM氏の所持しているクレジットカードを、この盗用防止システムに組込んだ場合につき説明する。インターネット内に設けた通報用電子郵便ステーション(INT)のドメイン名を「YYYY.COM」とし、M氏の通報用アドレスを「CCC」とした場合、このM氏の盗用防止用Eメールのアドレスは「CCC@YYYY.COM」となる。また、M氏の所有するポケットベルAを、ページングネットワークから通報できるポケットベルとしてユーザ登録し、該ポケットベルAと前記の通報用アドレス「CCC」とを対応付けておく。

【0010】M氏が自身のクレジットカードを使用した場合、或いは家族がM氏のクレジットカードを使用した場合、このクレジットカードが使用されたことと、その使用金額とが銀行Eのコンピュータに通報され、銀行Eのコンピュータは、M氏の盗用防止用Eメールをインターネットに自動送信する。Eメールの内容は、クレジットカードの種類(VISA, Master等)を表わす記号と、銀行Eのコード番号と、予め決められた通貨単位による使用金額であり、例えば、[A04] 20000という内容にアドレス「CCC@YYYY.COM」をつけてインターネットに送信する。

【0011】インターネット内に送信されたEメールは、そのドメイン名を持つサーバに送られる。このM氏の盗用防止用Eメールは、直ちに通報用電子郵便ステーション(INT)に届き、アドレスCCC宛の[A04] 20000という内容が届いた旨の通知が、通報用電子郵便ステーション(INT)からページングセンタ(PP)に通報される。ページングセンタ(PP)は、アドレスCCCが指し示すM氏所有のポケットベルAを呼出し、Eメールの内容[A04] 20000を送信してポケットベルAの表示部に表示させる。

【0012】M氏は、クレジットカードの取引後に鳴ったポケットベルAの表示を見ることで、自身或いは家族のクレジットカードによる取引が、VISAカード(記号A)による取引であり、銀行がコード番号04のXX銀行であり、金額が20000人民元であることを確認でき、この盗用防止システムが正常に機能していることを確認できる。

【0013】M氏のクレジットカードを不正に入手した他人がこのクレジットカードを用いて取引を行なった場合にも、上述したのと同様に、M氏所有のポケットベルAに情報が送信される。M氏は、ポケットベルAが作動して表示された内容を見ることで、自身のクレジットカードが盗難に遭っており、かつそれが現在不当に使用されている事実を直ちに知り得るものである。そこでM氏は、警察に通報すると共にカード会社にそのクレジットカードの停止を請求することが可能となる。

【0014】前述した実施例は、クレジットカードの盗用防止であったが、同じ盗用防止システムで携帯電話の盗用防止を図ることもできる。今、N氏所有の携帯電話を使って自身或いは家族が電話をかけたとする。この場合、電話会社のコンピュータFは、その携帯電話が使用されていることを示すメール内容「-222-」を、インターネットにN氏の盗用防止用Eメールアドレス「DD@YYYY.COM」を指定して自動送信する。このEメールはインターネットの通信網中を流れ、最終的に盗用防止の通報用サーバである電子郵便ステーション(INT; ドメイン名YYYY.COM)に到達する。ページングセンタ(PP)は、通報用電子郵便ステーション(INT)から通報を受け、N氏のアドレス「DDD」に対応するN氏所有のポケットベルBを呼出し、その表示部に携帯電話が使用されていることを示す「-222-」を表示する。N氏は、携帯電話の使用後すぐにポケットベルBに表示された内容を見て、この盗用防止システムが正常に動作していることを確認できる。

【0015】このN氏の携帯電話が他人に盗まれて、他人がN氏の携帯電話で通話した場合にも、前述と同様にN氏所有のポケットベルBに携帯電話の使用事実が表示される。この表示を見ることで、N氏は自身の携帯電話が盗まれて使用されていることを直ちに知ることができるので、N氏は警察に届けると共に電話会社に盗難に遭



った携帯電話の使用停止を請求できる。

【0016】先に述べた実施例は、クレジットカードと携帯電話の盗用防止に関するものであるが、前述した盗用防止システムはこれらの機器等の盗用防止に限られるものではなく、銀行小切手やマネーカード等の他の盗用防止対象物に対する盗用防止にも有効に適用できる。

【0017】

【発明の効果】以上に説明した如く、本発明に係る盗用防止方法およびそのシステムによればクレジットカードや携帯電話等に代表される盗用防止対象物の盗用を極め

て有効に防止できるものである。

【図面の簡単な説明】

【図1】本発明の一実施例に係る盗用防止システムの構成図である。

【符号の説明】

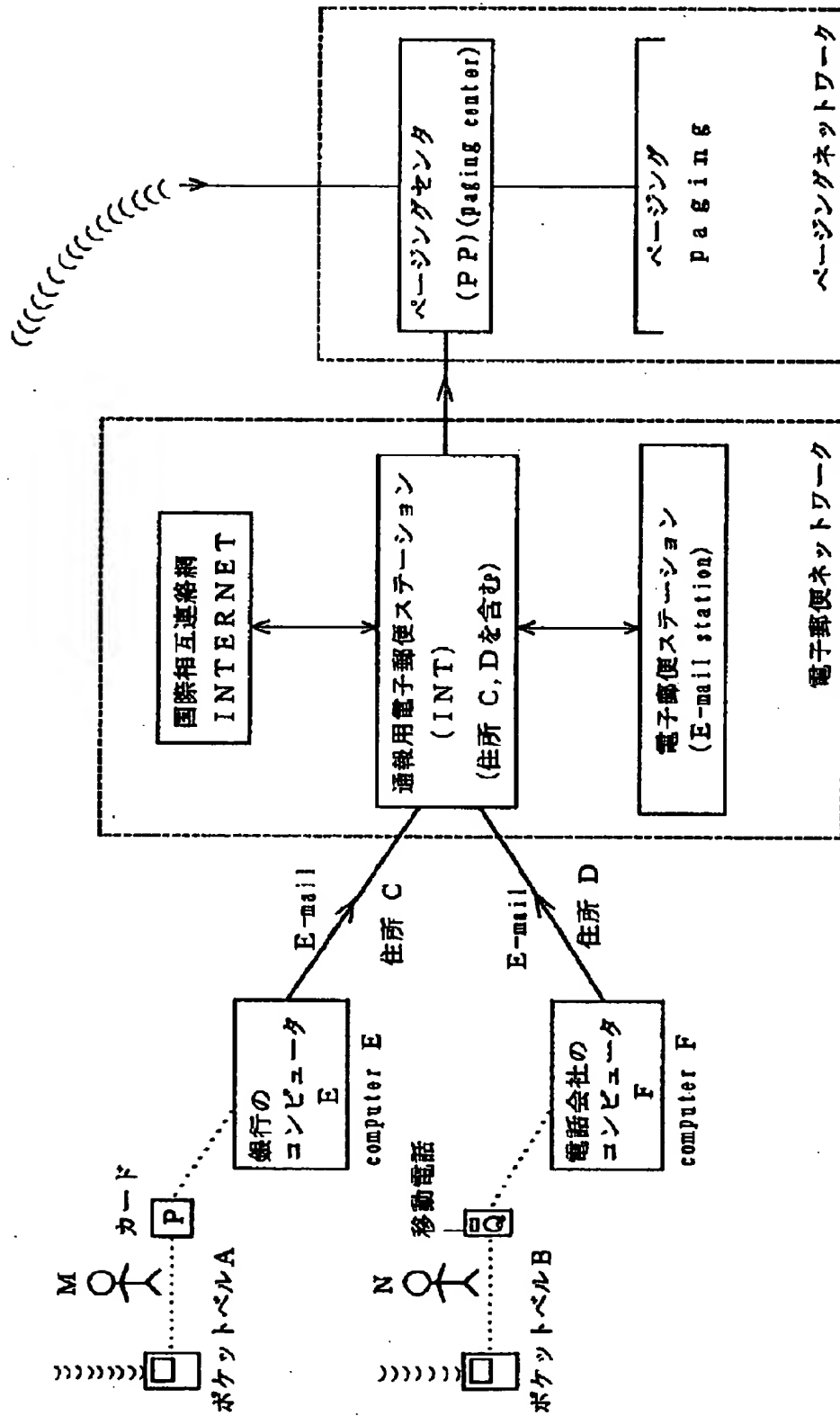
A, B ポケットベル

INT 通報用電子郵便ステーション

PP ページングセンタ

E, F コンピュータ

【図1】



フロントページの続き

(51) Int. Cl. <sup>6</sup>

識別記号

庁内整理番号

F I

技術表示箇所

H O 4 L 12/54

12/58

H O 4 M 3/42

1 0 2